

Prepared Statement of
Alan Davidson, Associate Director
The Center For Democracy & Technology
before
The Senate Committee On Commerce, Science, And Transportation
on
Consumer Privacy and
Government Technology Mandates in the Digital Media Marketplace

Wednesday, September 17, 2003

Mr. Chairman and members of the Committee, the Center for Democracy & Technology (CDT) is pleased to have this opportunity to speak to you about the difficult questions surrounding the expedited subpoena provision of the Digital Millennium Copyright Act (DMCA) and the enforcement of copyright online. CDT is a non-profit, public interest organization that is dedicated to promoting civil liberties and democratic values on the Internet. CDT is pleased to be part of today's hearing, both because of our long history of involvement in online privacy issues and our current efforts to craft a balanced consumer perspective on digital copyright.

We are at a critical moment in the evolution of digital copyright. Facing extensive unauthorized redistribution of their copyrighted material, recording companies have, for the first time, begun a large-scale campaign against individuals who the companies believe are infringing their copyrights online. While enforcement is unpopular, it is likely necessary. The question for this hearing is how to give copyright holders the tools they need to enforce their rights in the unique landscape of the digital world, while at the same time protecting the due process rights and privacy interests of individuals.

The expedited subpoena authority of the DMCA provides an important tool for copyright enforcement, but one that raises real privacy concerns for Internet users. We believe that with added safeguards a balance can be struck that gives users reasonable protections while ensuring that copyright owners are able to proceed against online infringers.

I wish to emphasize four key points in my testimony:

- Enforcement of copyright statutes is necessary to ensure that the balance that is enshrined in our copyright laws, between incentivizing creative production and facilitating its use, is translated into practice. It is unhealthy for our country, and unfair to copyright holders, for large numbers of people to routinely violate the law of the land.
- A subpoena process like that granted under Section 512(h) of Title 17, as amended by the Digital Millennium Copyright Act (DMCA), has an important role in assisting

enforcement, and with appropriate safeguards for individuals could be preferable to filing federal lawsuits.

- At the same time, serious privacy issues are raised by the unique subpoena power currently granted any copyright holder under 512(h), which too easily allows the identity of Internet users to be unmasked wrongly or by mistake, without the user's knowledge, without the possibility of redress, and without oversight.
- Much could be done to address the privacy concerns raised by Section 512(h) without getting in the way of the enforcement needs of copyright holders. Specifically, we support a notice requirement before subscriber identity is disclosed, and we suggest that Congress also consider sanctions for misuse, compensation for ISPs, reporting requirements, and limitations on use and retention of information. The changes we suggest are narrow and consistent with the main points of the DMCA.

The 512(h) issue is, of course, just one part of the much broader question of how best to protect copyright while protecting reasonable uses and encouraging innovation.

We note that there are many privacy issues raised by file trading and digital rights management beyond 512(h). For example, studies show that many peer-to-peer users inadvertently share personal information on their computers and that so-called "spyware" within some peer-to-peer applications creates serious privacy concerns. While this hearing is focused on 512(h) subpoenas, members of this Committee have been among the leaders in Congress on privacy issues, and we look forward to working with you to address these broader privacy concerns.

Mr. Chairman, CDT commends the efforts that you and this committee have made to address the important privacy questions raised by the use of Section 512(h) subpoenas. CDT believes a balanced approach is possible, and that Congress is the appropriate place for that balance to be struck.

I. The Need for Copyright Enforcement Online

Copyright holders face serious challenges in the online, digital world. With peer-to-peer file sharing networks and other powerful communications technologies at their disposal, Internet users are able to share content to a greater extent than ever before. While these technologies hold the potential to advance social discourse, transform content delivery, encourage creative production, and promote economic growth, they have, at the same time, allowed rampant copyright infringement that threatens the businesses of many content producers.¹

¹ While there is some debate about the exact contours of illegal infringement in the context of copying music on a computer, it seems clear that the behavior of many file-traders today violates the law.

Widespread use of the current generation of peer-to-peer programs, which do not include centralized servers, has forced copyright holders to go after infringing users themselves. In the last several months, the recording industry has started to do just that.

CDT supports copyright holders' ability to enforce their rights online, consistent with due process. It is important for consumers to have a copyright system that rewards authors and encourages the production of quality music, video, and other information goods. Determining the proper level and means of protection represents a delicate balancing act, but enforcement of existing statutes is necessary to ensure that legal balancing is translated into practice. It is essential that consumers and computer users understand the consequences of their actions online.

This summer's actions did not come without warning. We are encouraged by the RIAA's assurance that it is pursuing only "egregious" violators of copyrights. In its continuing legal efforts, we urge the RIAA to maintain a commitment to focus not on "de minimis" traders, but rather on those individuals who most clearly appear to have engaged in substantial violations of copyright law.

We believe the RIAA's continued legal offensive could have a rapid and significant effect in reducing the amount of infringement online, especially if it is coupled with attractive legal sources of digital music for consumers. These suits will send a clear, and unfortunately probably necessary, message that the content industry is serious about protecting its copyrights.

We believe that enforcement will be most effective if accompanied by legal, affordable alternatives and coupled with consumer education efforts. In the long run, cracking down on music piracy without providing attractive legal alternatives will only alienate consumers. And while the RIAA has done much to educate consumers already, the early reactions to the lawsuits filed last week demonstrate that many consumers still do not understand their rights and responsibilities under copyright law. The RIAA must share some of the responsibility in addressing this problem.

It is important that the music industry's enforcement efforts be viewed in the context of the ongoing policy debate about potential legal mandates for copy protection technology. Technology mandates raise extremely difficult issues regarding innovation and reasonable uses of copyrighted works. We note that the RIAA itself has chosen to pursue enforcement and new delivery models rather than call for new laws. CDT believes it makes sense to pursue enforcement of existing powerful copyright laws before pursuing controversial and difficult new technology mandates.

II. The Importance of an Expedited Subpoena Process

Technology has changed the target of copyright enforcement. On the Internet, millions of people are publishers. Because current peer-to-peer file-sharing networks do not include any centralized storage facility, the music industry cannot cut off the flow of copyrighted material

by suing a single centralized defendant. In order to address infringement occurring on these file-sharing networks, the industry is forced to go after individual consumers.

For this reason, it is easy to see why an expedited subpoena process could be an important tool for enforcement. Copyright enforcement ultimately relies on identifying end users thought to be in violation of copyright, even when the users are not storing any infringing material on an ISP's hardware. The number of actions required to effectively enforce copyright on peer-to-peer networks could be substantial. An expedited subpoena process allows copyright holders to contact suspected infringers without filing a federal lawsuit, a less costly approach for those enforcing copyright.

512(h) subpoenas do raise privacy and due process concerns for users, as we note below. For that reason many parties have argued that subscriber identity should only be revealed in the context of a federal "John Doe" lawsuit that provides additional judicial oversight for a third-party subpoena to get subscriber identity.

Provided appropriate safeguards are added to 512(h), it is not clear to us that suspected users would, in fact, be better off as defendants and targets of discovery actions in a federal lawsuit than as subjects of the much more limited disclosure allowed by the 512(h) subpoena. Even though they occur with judicial oversight, disclosures under a John Doe suit can be much more invasive, including financial data and surfing habits. An expedited subpoena process at least makes it possible for copyright holders to contact users – to notify them of suspected behavior, demand redress, or seek settlement – without setting in motion the machinery of filing a federal lawsuit against them.

III. Privacy Concerns Raised by 512(h) Subpoenas

While 512(h) subpoenas are a valuable element of enforcement, they also raise real privacy concerns. The 512(h) process allows the disclosure of private information with few protections against abuse or misuse. The efforts of Verizon and Pacific Bell to challenge Section 512(h) subpoenas have been instrumental in raising these issues.

Subscriber privacy is a cornerstone of commerce and communications online. People reasonably expect that their activities online can be anonymous or pseudonymous when they visit health information sites, make political statements, visit chat rooms, or become online whistleblowers. Revealing the identity of a person online can mean revealing that person's health status or political beliefs, what they read online or whom they socialize with. For that reason our law has strongly protected subscriber identity—placing, for example, serious restrictions on when ISPs can be forced to turn that information over to the government.

512(h) allows a broad category of private parties to avail themselves of the awesome power of the federal courts to compel ISPs to divulge this private and sensitive piece of information. Among the privacy concerns raised by 512(h) are:

- *Breadth of potential use:* Section 512(h) permits any copyright holder, literally millions of people and organizations, to compel disclosure of subscriber information based on a mere allegation of copyright infringement. Use of the subpoenas need not be confined to the enforcement of copyright by mainstream recording companies or movie studios. For example, Titan Media’s recently publicized attempt to uncover the identity of 59 alleged traders of gay pornography raises clear concerns about the disclosure of people’s identities in the context of sensitive or private activities online. And as the National Network to End Domestic Violence pointed out in a letter to the Senate Judiciary Committee last week, even more malicious uses of the subpoena process by criminals are possible.
- *No notice to end-users:* The disclosure of personally identifying information takes place without the requirement of any notice to the end user that his or her identity has been unmasked. People typically have no idea that their personal information is being revealed. Notice has long been a bedrock of our privacy law because it gives the party actually aggrieved—and in the best position to assess whether information was given out improperly—the ability to combat misuse.²
- *Lack of redress:* If the subpoena process is misused, 512(h) provides no meaningful opportunity for users to seek redress. While some elements of 512(h) applications are made “under penalty of perjury,” other elements are not, and the faint prospect that a U.S. Attorney will actually prosecute someone who lies on his application is likely to be of little comfort to users. Congress clearly understood this issue as Section 512(f) does provide for damages based up on misrepresentation, but only for damages that are the “result of the service provider relying upon such misrepresentation in removing or disabling access” to material. Thus even the penalties that Congress put in place for misuse in 512(f) do not apply to inappropriate disclosure of identity under 512(h).
- *No judicial oversight:* No judge ever looks at a 512(h) application, no weighing of facts is ever made beyond the assertions in the application, and no user ever gets to challenge those assertions.
- *No confidentiality requirement or limitations on future use of data:* There is little effective limitation on how the information disclosed in compliance with a 512(h) subpoena will be used. Can it be kept forever? Can it be used to blacklist, embarrass, market to, or harass alleged infringers? The law places no real limits beyond the open-ended requirement that information be used for “protecting rights.”

512(h) is unique in that it allows a broad category of private actors to obtain sensitive information from third parties, outside of the context of litigation. Private use of the courts in this way almost always takes place in the context of litigation or pending litigation, and under the supervision of a judge able to assess facts and to balance the interests at stake.

² Nothing in 512(h) expressly precludes ISPs from giving their subscribers notice. However, from a user perspective, many ISPs do not give such notice, the cost for providing notice could be high in large numbers, and notice might not be given in a timely fashion—all making a notice requirement attractive.

Many provisions exist for government access to information—but in the context of its executive powers, and in almost all cases with additional and constitutionally mandated privacy protections. For example, the Right to Financial Privacy Act allows the federal government to access financial records through an administrative subpoena process only if notice is given to consumers and no motion to quash is filed within the next fourteen days.³ And both the Cable Communications Policy Act and the Video Privacy Protection Act require that notice be provided to consumers before a court issues any order requiring cable providers or video rental services to provide consumer information to the government.⁴

These concerns have formed the basis of ongoing legal challenges to 512(h). CDT is sympathetic to many of the Constitutional concerns raised in those lawsuits, but we also believe this issue is a classic instance of balancing interests and—consistent with Constitutional requirements—is ultimately best resolved by Congress.

IV. Protecting Privacy, Preserving Enforcement in the 512(h) Process

We believe that many of the privacy shortcomings of 512(h) can be remedied with relatively minor changes that do not impede—and may in fact promote—enforcement goals. Existing privacy laws suggest a number of legislative tools that could enhance privacy and due process without sacrificing 512(h) enforcement benefits. We highlight five areas for improvement, the first of which—notice—we believe is most essential, but which may not be sufficient alone.

- *Notice:* Formal notification that they are the targets of a subpoena would give people warning that their personal information is being given out, and put them in a position to contest wrongful subpoenas. Ideally notice would be given both electronically and by mail by an ISP, and would provide users with a meaningful opportunity to quash a subpoena that is wrongfully issued. For example, in the context of tort lawsuits, Virginia state law requires that ISPs provide notice to an anonymous Internet user at least 30 days before releasing his or her identity to a subpoenaing party.⁵ While Congress may determine that 30 days is too long a period in the context of digital copyright infringement, some prior notice would be valuable to protect end user privacy.⁶ Notice can have a substantial deterrent effect on abuse because subpoena applicants would know that their targets would hear of their requests, and would be able to seek court protection if they were improper.

³ 12 U.S.C. § 3405(2), 3407(2).

⁴ 47 U.S.C. § 551(h)(2); 18 U.S.C. § 2710(b)(3).

⁵ 8.01 Va.C. § 407(1).

⁶ Deferred notice—providing notice after identity has been released—might minimize impacts on enforcement but is a second-best solution for users who would have no opportunity to challenge a mistaken or wrongful subpoena. Alternatively, deferred notice could be granted under special circumstances after review by a judge.

A notice requirement would also help legitimate copyright enforcement. Official notification that they are the targets of legal investigation would in many cases be enough to make users stop infringing behavior, and would strengthen deterrence by increasing people's awareness of legal actions. It is our understanding that the risk of disrupting investigations by "tipping off" suspects is minimal; copyright holders collect evidence of infringement before even applying for a subpoena, so little is lost by notifying a suspect that a subpoena is being issued.

- *Penalties for abuse:* End users should be entitled to damages if a subpoenaing party misuses identifying information once revealed, as well as in cases where ISPs fail to provide notice when complying with a subpoena request. One good model can be found in a draft bill under active consideration in the California state legislature that provides damages to people whose identities are revealed by their ISPs, if that information is misused.⁷ This requirement places little or no additional burden on parties using the subpoena process for legitimate enforcement goals, but imposes real penalties on those who would take advantage of the process. Congress appears to have complemented similar redress in Section 512(f)'s damages for misrepresentation, which as we note do not apply to damages from improper subpoenas.
- *Cost reimbursement:* From a consumer perspective, requiring subpoenaing parties to reimburse for costs of compliance with their subpoenas can serve as a check against frivolous subpoena requests. Federal Rule of Civil Procedure 45, or the Virginia law on subscriber identification, provides good examples of cost reimbursement.
- *Reporting requirement:* A major problem with 512(h) is that the public has no idea how often the provision is being used. An annual report to Congress on the number of subpoenas requested and granted would provide valuable oversight about how often and in what way the 512(h) process is being used, and would be a first step in monitoring for potential abuses.
- *Limitation on use and retention of information:* The purpose to which information obtained in a 512(h) subpoena can be used could be clarified, and a definite time limit established for which the information could be retained. With a sufficiently long time retention period – on the order of several years – this requirement should make little difference for parties using the subpoena process to pursue real enforcement goals, but would alleviate end-user concerns about the ways in which their personal information might be used over time.

All five of these approaches represent places where important protections for users can be introduced without burdening enforcement.

⁷ "Internet Communications Protection Act of 2003," Cal. AB 1143 (2003).

V. Conclusion

We believe enforcement of existing copyright law, with appropriate safeguards, is a sensible and necessary part of dealing with the problems posed by digital piracy. Enforcement is also preferable—if it can be made effective—to undertaking the difficult task of crafting new legislation on the issues of technology mandates. For this reason we think it is important that copyright holders have the information necessary for meaningful enforcement, subject to adequate safeguards.

At the same time, Section 512(h) raises serious privacy concerns for users, particularly as interpreted by the courts to date. We believe that with relatively minor additional safeguards, many of these privacy concerns can be addressed while preserving – and in some ways enhancing – legitimate enforcement efforts.

We commend the Chairman and members of this committee for raising awareness of the real privacy issues that are raised by Section 512(h) subpoenas. We look forward to working with this committee, the industry, and others in the public interest community to craft a more balanced approach to the 512(h) subpoena issue.